Available online at www.sciencedirect.com
ScienceDirect
Theoretical Computer Science 380 (2007) 355–362
Theoretical Computer Science
www.elsevier.com/locate/tcs

Extension of the decidability of the marked PCP to instances with unique blocks

Vesa Halava[a,*], Tero Harju[a], Juhani Karhumäki[a], Michel Latteux[b]

[a] *Department of Mathematics and Turku Centre for Computer Science, University of Turku, FIN-20014 Turku, Finland*
[b] *Université des Sciences et Technologies de Lille, Bâtiment M3, 59655 Villeneuve d'Ascq Cédex, France*

Abstract

In the Post Correspondence Problem (PCP) an instance (h, g) consists of two morphisms h and g, and the problem is to determine whether or not there exists a nonempty word w such that $h(w) = g(w)$. Here we prove that the PCP is decidable for instances with unique blocks using the decidability of the marked PCP. Also, we show that it is decidable whether an instance satisfying the uniqueness condition for continuations has an infinite solution. These results establish a new and larger class of decidable instances of the PCP, including the class of marked instances.

Keywords: Post Correspondence Problem; Infinite Post Correspondence Problem; Marked morphism; Unique continuation; Unique block; Decidability

1. Introduction

In the *Post Correspondence Problem* (PCP, for short), we are given two morphisms $h, g\colon A^* \to B^*$, where A and B are finite alphabets, and we are asked whether or not there exists a nonempty word $w \in A^*$ such that $h(w) = g(w)$. The pair (h, g) is called an *instance* of the PCP and a word $w \in A^+$ is a *solution* of the instance (h, g) if $h(w) = g(w)$. The set of all solutions,

$$E(I) = \{w \in A^+ \mid h(w) = g(w)\},$$

is called the *equality set* of the instance $I = (h, g)$. The *size* of an instance I is $|A|$, that is, the cardinality of the domain alphabet of the morphisms.

The PCP is a well-known problem which was proved originally to be undecidable by Post [13]. In the theory of undecidability one central topic is to investigate the borderline between decidability and undecidability. This is often done by choosing a known undecidable problem, like the PCP, and then setting further restrictions to the instances of the problem, which possibly cause the problem to be decidable. In the PCP this borderline has been investigated

* Corresponding author. Tel.: +358 2 333 5617; fax: +358 2 333 6595.
E-mail addresses: vehalava@utu.fi (V. Halava), harju@utu.fi (T. Harju), karhumak@utu.fi (J. Karhumäki), latteux@lifl.fr (M. Latteux).

0304-3975/$ - see front matter
doi:10.1016/j.tcs.2007.03.024

in several ways. For example, it is an easy exercise to show that the unary PCP, where the domain alphabet has only one letter, is decidable. It is highly nontrivial to show that the PCP is decidable for binary instances (i.e. of size 2). This was proved by Ehrenfeucht, Karhumäki and Rozenberg [1]; see also [5] or [6] for a somewhat simpler proof. On the other hand, the PCP is undecidable for instances of size at least seven as was shown by Matiyasevich and Sénizergues [12].

Another known boundary line of decidability is provided by marked and prefix morphisms. A morphism $h\colon A^* \to B^*$ is said to be *marked* if the images $h(a)$ and $h(b)$ of any two different letters $a, b \in A$ begin with different letters. It was proved by Halava, Hirvensalo and de Wolf [9], that the PCP is decidable for marked instances. On the other hand, Lecerf [11] showed that the PCP is undecidable for instances of injective morphisms, and Ruohonen [14] proved the undecidability for instances of (bi)prefix morphisms, where no image of a letter is a prefix of an image of another letter. Note that both marked and prefix morphisms are special cases of injective morphisms.

In this paper we study instances of the PCP, which are not necessarily marked, not even injective, but they can be reduced to marked instances of the PCP. These instances satisfy the so called unique block condition. We also study infinite solutions of the instances (h, g) satisfying the condition called unique continuation.

Two (finite) words u and v are said to be *comparable*, if one is a prefix of the other. Let $\omega = a_1a_2\cdots$ be an infinite word over A where $a_i \in A$ for each index $i = 1, 2, \ldots$. Note that $h(\omega) = g(\omega)$ if $h(u)$ and $g(u)$ are comparable for all finite prefixes u of ω. We also say that such an infinite word ω is an *infinite solution* of the instance (h, g).

The problem whether or not a given instance of the PCP has an infinite solution is called naturally the *infinite PCP*, or *ωPCP*, for short. It was shown by Ruohonen [14] that there is no algorithm to determine whether a general instance of the PCP has an infinite solution. On the other hand, it was proved in [3] that the ωPCP is decidable for marked instances of the PCP. Later, using the previous result, it was shown in [7] that the ωPCP is decidable for binary instances. Recently, it was proved in [4] that the ωPCP is undecidable for instances of size 9.

It seems that the unique block condition is not enough to make the ωPCP decidable, but when we use the sharper condition of unique continuation, the ωPCP turns to be decidable.

We shall now fix some notation. The *empty word* is denoted by ε. The length of a word u is denoted by $|u|$. A word $u \in A^*$ is said to be a *prefix* of a word $v \in A^*$, denoted by $u \le v$, if $v = uw$ for some $w \in A^*$. Also, if $u \neq \varepsilon$ and $w \neq \varepsilon$ in $v = uw$, then u is a *proper prefix* of v, denoted by $u < v$. Recall that u and v are comparable, denoted by $u \bowtie v$, if $u \le v$ or $v \le u$. If $v = uw$ then we also write $u = vw^{-1}$ and $w = u^{-1}v$. A word $u \in A^*$ is said to be a *suffix* of a word $v \in A^*$, if $v = wu$ for some $w \in A^*$. If $u \neq \varepsilon$ and $u \neq v$, then the suffix u is *proper*.

2. Unique block instances

Recall that a morphism $h\colon A^* \to B^*$ is marked if the images $h(a)$ and $h(b)$ do not have a common nonempty prefix for any pair of different letters $a, b \in A$. The basic result on which we build the results of this paper is the following theorem from [9]; see also [2]:

Theorem 1. *The PCP is decidable for marked instances of any size.*

We aim at a decision procedure for special instances of the PCP. However, we start with a simpler problem:

> **Problem 1.** Let $b \in B$ be a fixed letter. Given a marked instance $I = (h, g)$ of the PCP, where $h, g\colon A^* \to B^*$. Does there exist words $x, y \in A^+$ such that $h(x) = g(y)$ and $b \le h(x)$?

In this problem we do not look for solutions for the equation $h(x) = g(x)$, but rather for $h(x) = g(y)$ together with the addition requirement that $h(x)$ should begin with the specified letter b. This problem is known to be decidable for arbitrary pairs of morphisms, the reasoning being that the language $h(A^*) \cap bB^*$ is regular, and required words x and y exist if and only if

$$\big(h(A^*) \cap bB^*\big) \cap \big(g(A^*) \cap bB^*\big) \neq \emptyset, \tag{1}$$

where emptiness can be decided since it concerns regular languages.

The basic notion in the proof of Theorem 1 is that of a block. Let $h, g\colon A^* \to B^*$ be nonerasing morphisms, i.e., $h(a) \neq \varepsilon$ and $g(a) \neq \varepsilon$ for all letters a. A pair (u, v) is a *block* (*for the letter* b) of the instance (h, g), if $h(u) = g(v)$ and $h(u') \neq g(v')$ for all proper prefixes $u' < u$ and $v' < v$ with $b \le h(u)$. In this case, u and v are called *block words*. Denote by $S_b(h, g)$, or simply by S_b, the set of all blocks for the letter b.

Table 1
An instance (h, g) of nonmarked morphisms satisfying (UC1)

	a	b	c	d
h	ab	abc	$cccc$	b
g	a	$babc$	cc	bbc

Table 2
An instance (h, g) satisfying the (UC1) condition

	a	b	c	d
h	a	ba	$cabbb$	ab
g	ac	bac	$abbb$	c

If (u, v) is a solution of the equation $h(x) = g(y)$, then there exist decompositions $u = u_1u_2 \cdots u_k$ and $v = v_1v_2 \cdots v_k$ of u and v such that $(u_i, v_i) \in S_{b_i}$ for some letters for $b_i \in B$, $i = 1, 2, \ldots, k$. Thus if $u = w = v$ is a solution of an instance (h, g), there exists a *block decomposition* of w,

$$w = u_1u_2 \cdots u_k = v_1v_2 \cdots v_k, \tag{2}$$

where $(u_i, v_i) \in S_{b_i}$ for $b_i \in B$, $i = 1, 2, \ldots, k$, i.e. each solution can be represented as a concatenation of blocks.

For a marked instance (h, g), the block for every letter b is unique, if it exists, and, therefore, in the marked case every solution has a unique block decomposition (see [9] or [2]).

Let us now define the first unique continuation condition:

UC1. The instance (h, g), where $h, g\colon A^* \to B^*$, is called a *unique block instance* if, for every letter $a \in A$, there exist at most one block (au, v) and at most one block (u, av).

If an instance $I = (h, g)$ satisfies (UC1), and if (u, v) is a block, where $a \le u$ for a letter $a \in A$, then we denote

$$\beta(a) = (u, v).$$

Example 1. We give an example of a unique block instance for non-marked morphisms. Let $h, g\colon \{a, b, c, d\}^* \to \{a, b, c\}^*$ be the morphisms defined in Table 1.

This instance satisfies (UC1). The blocks are (ab, ab), (c, cc) and (db, b). For example, $h(adc^i) \bowtie g(adc^j)$ and $h(aac^i) \bowtie g(abc^j)$ for all i and j, but there is no block of the form (adc^i, adc^j) or (aac^i, abc^j). Clearly, $w = ab$ is a solution of the PCP and $\omega = adc^\omega$ is a solution of the ωPCP for this instance.

Example 2. We give another example of a unique block instance, where the morphisms are defined in Table 2.

In this example, h is not injective, since, for example, $h(ab) = aba = h(da)$. On the other hand, the instance (h, g) satisfies (UC1) the blocks being (ac, ac), (bc, bc) and (c, dc). We conclude that the class of instances with unique blocks does not consist of injective morphisms only.

Note that the instances satisfying the condition

$$|S_b| \le 1, \tag{3}$$

for all $b \in B$, form a subclass of the instances satisfying (UC1). Note also that the marked instances satisfy condition (3).

We show now that the condition (UC1) ensures reduction to marked instances. First of all, it is obvious that all solutions of an instance of the PCP have a unique block decomposition. This is clear, since all images of solutions can be divided into a minimal factors, which are equal in the images of both morphisms. These are clearly the blocks.

For the instances satisfying (UC1), the uniqueness of the blocks for each starting letter gives a reduction of the instances to the marked instances. Moreover, the condition (UC1) yields that the constructive search for a solution is deterministic with respect to the blocks. Indeed, assume that the instance $I = (h, g)$, where $h, g\colon A^* \to B^*$, satisfies (UC1), and suppose that $w \in A^+$ is a solution of I. Let $w = u_1u_2 \cdots u_k = v_1v_2 \cdots v_k$, where each $(u_i, v_i) = \beta(a_i)$ is a block for some $a_i \in A$. In particular, $u_i = a_iu_i'$ for some u_i'. It is clear that such a decomposition always exists for all solutions. For the first letter $a_1 \le w$, the block (a_1u_1', v_1) is unique by (UC1). Furthermore, for all $i \ge 2$, $a_i \le (u_1 \cdots u_{i-1})^{-1}w$ and therefore also the block $(u_i, v_i) = (a_iu_i', v_i)$ is unique by (UC1).

The next theorem is our first main result for instances satisfying (UC1).

Theorem 2. *The PCP is decidable for unique block instances.*

Proof. Assume that the instance $I = (h, g)$, where $h, g\colon A^* \to B^*$, satisfies the condition (UC1). We construct a marked instance $I' = (h', g')$, where $h', g'\colon C^* \to A^*$, as follows. Let

$$C = \{a \in A \mid \beta(a) \text{ exists}\}\,.$$

For each $a \in C$, let $\beta(a) = (u, v)$, and define

$$h'(a) = u \quad \text{and} \quad g'(a) = v.$$

Clearly, the morphisms h' and g' are marked by the condition (UC1). Note also that $a \le h'(a)$ for all $a \in C$.

We prove that I' has a solution if and only I has. Indeed, assume that I has a solution w, and let

$$u_1u_2 \cdots u_k = w = v_1v_2 \cdots v_k$$

be its block decomposition, where $(u_i, v_i) = \beta(a_i)$, with $a_i \in A$, $i = 1, \ldots, k$. This decomposition is unique, and, for $w' = a_1a_2 \cdots a_k$, we obtain

$$h'(w') = u_1u_2 \cdots u_k = w = v_1v_2 \cdots v_k = g'(w'),$$

and therefore w' is a solution of I'.

In converse, assume that I' has a solution $w' = a_1a_2 \cdots a_k$, $a_i \in C$ for all i. Now

$$w = h'(w') = u_1u_2 \cdots u_k = v_1v_2 \cdots v_k = g'(w'),$$

where $h'(a_i) = u_i$, $g'(a_i) = v_i$ and $(u_i, v_i) = \beta(a_i)$. By the definition of block, $h(u_i) = g(v_i)$ for all i and, therefore,

$$h(h'(w')) = h(u_1u_2 \cdots u_k) = g(v_1v_2 \cdots v_k) = g(g'(w')).$$

In other words, $h'(w')$ is a solution of I.

The result follows now from Theorem 1. □

Note that in the proof of previous theorem, in order for both h' and g' to be marked, we need the fact that in the instances satisfying (UC1) every letter of $a \in A$ is the first letter of at most one block of both h and g.

An effective decision procedure for the instances satisfying (UC1) uses the same techniques as the algorithm for the marked instances given in [9]. Indeed, for a marked instance $I = (h, g)$, the *successor* $I' = (h', g')$ is build as in the proof of Theorem 2. By iterating the successor construction, the *successor sequence* $I^{(i)} = (h^{(i)}, g^{(i)})$, $i = 1, 2, \ldots$, is obtained. The conclusion is that this sequence is ultimately periodic, that is, there exist numbers n and d such that $I^{(i)} = I^{(i+d)}$ for all $i \ge n$. Finally, there exists a solution beginning with a letter a for I if and only if $h^{(i)}(a) = a = g^{(i)}(a)$ for all $i \ge n$. We refer to [9] for more detailed proofs concerning this decision procedure. Note that for a marked instance I the letters for which a minimal solution exists, can be detected, and also the minimal solution for each letter is unique, that is

$$E_{\min}(I) = E(I) \setminus E(I)^2 = \{w_1, w_2, \ldots, w_k \mid w_i \text{ is the minimal solution for letter } a_i,\ 1 \le i \le k\}\,.$$

Now by the proof of Theorem 2, we obtain:

Corollary 1. *Let $I = (h, g)$ be a unique block instance of the PCP and assume that the domain alphabet is A. The following sets can be effectively found:*

(1) $S = \{a \in A \mid$ *there exists a solution w for I, $a \le w$*$\}$
(2) $E_{\min}(I)$ *is a finite marked set effectively computable. Marked here means that every element of $E_{\min}(I)$ begins with a different letter.*

In order to make use of Theorem 2, we must be able to prove that we may detect the unique block instances. Therefore, we need to prove

Theorem 3. *It is decidable, whether or not an instance (h, g) of the PCP is a unique block instance.*

Proof. We establish a procedure for deciding whether or not an instance is a unique block instance.

Let $I = (h, g)$, where $h, g\colon A^* \to B^*$, be an instance of the PCP. For a letter $a \in A$, construct the minimal deterministic finite automata accepting the regular language

$$H_a = h(aA^*) \cap g(A^*).$$

This can be done by the usual tricks in the theory of finite automata, by first defining automata for languages $h(aA^*)$ and $g(A^*)$, and then using the construction in [10] for intersection. The minimal automaton $\mathcal{A}$ can be found with so called *The Method of Quotients* in [10]. Now there exists a unique block (au, v) of I for the letter a only if $\mathcal{A}$ is not *branching* before it reaches a final state for the first time, that is, there is a unique path from the initial state to a final state consuming a word $w_a \in H_a$. We still need to check that the word au satisfying $h(au) = w_a$ is unique. This can be checked simply by examining all possible factorizations of w_a by images of h. Similarly, we have to check that w_a has a unique factorization with images of g, that is, v is the only such word that $g(v) = w_a$. Now, if au and v are unique for w_a, then (au, v) is unique for a.

Symmetrically, we can check whether or not blocks (u, av) are unique (if it exists) for every a. □

3. Unique continuation instances

The property (UC1) does not help in the ωPCP, since no reduction to marked instances of the ωPCP can be established. Indeed, a unique block instance can have an infinite solution without block decomposition and still be nonultimately periodic. For the ωPCP we need a stronger unique continuation condition to have a decidable ωPCP.

> **UC2**. An instance (h, g), where $h, g\colon A^* \to B^*$ is called a *unique continuation instance*, if whenever $h(u) < g(v)$ or $g(v) < h(u)$ for $u, v \in A^*$, then there exists at most one letter a such that $h(ua) \bowtie g(v)$ or $h(u) \bowtie g(va)$, respectively.

It is obvious that a unique continuation instance needs not be injective. This can be seen, for instance, by taking any unique continuation instance (h, g) and adding there new domain letters a and b and setting $h(a) = a = h(b)$ and $g(a) = b = g(b)$. The new instance is still a unique continuation instance, but it is not injective.

We first prove that unique continuation instances can be effectively detected.

Theorem 4. *It is decidable, whether or not an instance of the PCP is a unique continuation instance.*

Proof. Let $I = (h, g)$, where $h, g\colon A^* \to B^*$, be an instance of the PCP. We define the following procedure called CONTINUATION. The input is (a, h, g), where $a \in A$.

(1) Set $i = 1$, $x_1 = a$ and $y_1 = \varepsilon$, $S_g = S_h = \emptyset$.
(2) If $h(x_i) = g(y_i)$, then return UNIQUE: CASE 1.
(3) Else if $g(y_i) < h(x_i)$, then if $s_i = g(y_i)^{-1}h(x_i) \in S_h$ return UNIQUE: CASE 2. Else set $S_h := S_h \cup \{s_i\}$.
If the letter b such that $g(y_i b) \bowtie h(x_i)$ is unique, then set $x_{i+1} = x_i$, $y_{i+1} = y_i b$ and $i = i + 1$, GOTO 2. If no such b exists, return NO BLOCK. Else return NOT UNIQUE.
(4) Else if $h(x_i) < g(y_i)$, then if $s_i = h(x_i)^{-1}g(y_i) \in S_g$ return UNIQUE: CASE 2. Else set $S_g := S_g \cup \{s_i\}$.
If the letter b such that $h(x_i b) \bowtie g(y_i)$ is unique, then set $y_{i+1} = y_i$, $x_{i+1} = x_i b$ and $i = i + 1$, GOTO 2. If no such b exists, return NO BLOCK. Else return NOT UNIQUE.

We shortly explain the idea of the procedure CONTINUATION. For an input letter a a sequence (x_i, y_i) is constructed, where $h(x_i) \bowtie g(y_i)$ for all i. The pair (x_{i+1}, y_{i+1}) is constructed using the *suffix overflow* $h(x_i)^{-1}g(y_i)$ or $g(y_i)^{-1}h(x_i)$ of the pair (x_i, y_i), according to whether $|g(y_i)| > |h(x_i)|$ or not. Uniqueness of the next letter is checked at every round. If the overflow is empty, then there is a (unique) block for the letter a. On the other hand, it is possible that the overflow is always nonempty. In this case, if the sequence (x_i, y_i) is infinite, the overflows begin to appear cyclically, and we may stop when find the first overflow twice. The sets S_h and S_g are used to check whether an overflow already appeared.

Now an instance satisfies condition (UC2) if and only if, for all $a \in A$, the procedure CONTINUATION returns UNIQUE for both inputs (a, h, g) and (a, g, h). Indeed, if CONTINUATION returns UNIQUE for all these input, then the continuation is unique for all overflows of the length at most $\max_{a\in A}\{|h(a)|, |g(a)|\}$, and this is enough. □

The following theorem holds, since a unique continuation instance necessarily satisfies (UC1). Indeed, the procedure CONTINUATION can be easily transformed into a procedure which detects unique blocks also, simply by returning the pair (x_i, y_i) if the procedure stop in the command line (2).

Theorem 5. *The PCP is decidable for unique continuation instances.*

The difference between unique block instances and unique continuation instances is that in the former case we may find several letters for each suffix overflow in the lines (3) and (4) of the procedure CONTINUATION, but the equality $h(x_i) = g(y_i)$ is eventually satisfied only for one choice of the letters. But in the unique continuation instances the choice of the next letter is always deterministically determined w.r.t. the suffix overflow. Using this deterministic behaviour, we are able to prove that the ωPCP is decidable for the unique continuation instances the proof of which uses the idea of [3] for the proof of the next theorem.

Theorem 6. *The ωPCP is decidable for marked instances.*

We are ready to prove our main theorem on ωPCP.

Theorem 7. *The ωPCP is decidable for the unique continuation instances.*

Proof. Assume that $I = (h, g)$, where $h, g\colon A^* \to B^*$, is a unique continuation instance. We can assume that $E(I) = \emptyset$, since for any nonempty $w \in E(I)$, $w^\omega = ww\cdots$ is an infinite solution of I and we are done.

We say that an infinite solution $\omega \in A^\omega$ has a block decomposition, if

$$\omega = u_1u_2\cdots = v_1v_2\cdots, \tag{4}$$

where each (u_i, v_i) is block for some letter a_i for $i = 1, 2, \ldots$. The infinite solutions of I are of two types, either they have a block decomposition, or they do not have a block decomposition. We prove that the infinite solutions of both types can be detected.

Assume first that I has a solution with a block decomposition, and let $I' = (h', g')$ be constructed as in the proof of Theorem 2. It is easy to show that there exists an infinite solution ω with block decomposition in (4) for I if and only if $\omega' = a_1a_2\cdots$ is an infinite solution of the marked instance I'. Since the ωPCP is decidable for marked instances (see Theorem 6), a solution with a block decomposition can be effectively found. Note also that, for any infinite solution ω' of the instance I', $h'(\omega')$ is an infinite solution of I.

The harder case consists of the instances I without block decompositions. Assume that ω is an infinite solution of I, that is,

$$\omega = u_1u_2\cdots u_k\omega_1 = v_1v_2\cdots v_k\omega_2, \tag{5}$$

where (u_i, v_i) are blocks for $i = 1, 2, \ldots, k$ and $\omega_1, \omega_2 \in A^\omega$ such that k is maximal with respect to this property, i.e. ω_1 and ω_2 do not have block words as prefixes. We shall describe a procedure which detects these infinite solutions.

By the maximality condition and the condition (UC2), both ω_1 and ω_2 begin with a letter for which no block exists. Clearly, such letters are those for which the procedure CONTINUATION returns “unique: case 2”. In this case, a suffix overflow repeats in the process, and, since I is a unique continuation instance, the suffix overflows appear periodically. Assume, that $(x_i, y_i) = (u, u')$ is the pair when the first repeated suffix overflow appears the first time, and $(x_j, y_j) = (uv, u'w)$ is the pair when the same overflow appears the second time. It is immediate that $h(uv^\omega) = g(u'w^\omega)$. Therefore, $\omega_1 = uv^\omega$ and $\omega_2 = u'w^\omega$ for some letters $b \leq uv$ and $c \leq u'w$ and for any block (x, y), $b \not\leq x$ and $c \not\leq y$. We have achieved that all possible ω_1 and ω_2 can be effectively determined. For each letter for which there is no block, we construct the words ω_1 and ω_2 if they exist. Note that we check also whether or not $\omega_1 = \omega_2$ which would immediately imply that ω_1 is an infinite solution.

We still need to prove that for all a_1 the block part $(u_1u_2\cdots u_k, v_1v_2\cdots v_k)$ in (5) can be effectively found. The bound k must be finite, since the instance does not have a block decomposition beginning with a_1. We construct the words $u_1\cdots u_k$ and $v_1\cdots v_k$ using the same idea as in the procedure CONTINUATION. Clearly, there exists a solution (5) if and only if either

$$(u_1u_2\cdots u_k)^{-1}(v_1v_2\cdots v_k) = cz \quad \text{or} \quad (v_1v_2\cdots v_k)^{-1}(u_1u_2\cdots u_k) = bz$$

for some letters b and c, and a word z, according to whether $|u_1 \cdots u_k| < |v_1 \cdots v_k|$ or not. Our algorithm works as the CONTINUATION for (a_1, h, g), but the sequence (x_i, y_i) is constructed so that in each step we check that $x_i \bowtie y_i$. If at some step i, x_i and y_i are not comparable, there is no infinite solution for a_1. Similarly, if CONTINUATION returns "no block", that is, no next letter for x_i or y_i exists and $h(x_i) \neq g(y_i)$. Now if CONTINUATION stops in the case $h(x_i) = g(y_i)$ (and $x_i \bowtie y_i$), we have that $x_i = y_i dz$ or $y_i = x_i dz$, for some letter d and a word z. In the first case, if there is a block word for g beginning with d, we set $x_{i+1} = x_i$ and $y_{i+1} = y_i d$, and continue according to the procedure CONTINUATION. Otherwise, there is no block word for g beginning with d, and $x_i = u_1 \cdots u_k$ and $y_i = v_1 \cdots v_k$. In the other case, where $y_i = x_i dz$, we reason similarly. Note that $dz \neq \varepsilon$, since $E(I) = \emptyset$. Since there is no infinite solution with a block decomposition, this algorithm necessarily stops eventually.

Finally, we need to check whether or not for the letter d there are infinite words $\omega_1 = uv^\omega$ and $\omega_2 = u'w^\omega$ as above, and that

$$u_1 u_2 \cdots u_k u v^\omega = v_1 v_2 \cdots v_k u' w^\omega.$$

These words are ultimately periodic and, therefore, their equality can be determined in a trivial way. □

The structure of the infinite solutions of the marked instances of the PCP was studied in detail in [8], and the infinite solutions of the unique continuation instances have the same structure. Indeed, it was proved in [8] that the set of infinite solutions for the marked instances I is of the form

$$E_{\min}(I)^\omega \cup E_{\min}(I)^* (P \cup F), \tag{6}$$

where P is a finite set of ultimately periodic words, and F is a finite set of morphic images of fixed points of D0L systems. In the proof of Theorem 7 it was shown that the solutions with a block decomposition are morphic images of solutions of a marked instance, and the solution without a block decomposition are ultimately periodic. Since the morphic images of ultimately periodic words in P are ultimately periodic and the morphic images of morphic images of F are of the type F, we obtain that

Theorem 8. *The infinite solutions of an instance of the PCP with unique continuation property have the structure of* (6).

Note that we could extend these properties to morphisms which satisfy the same condition from the right to left. Actually, if the condition (UC1) (or (UC2)) are satisfied for the mirror instance (h^R, g^R) of (h, g) where, for all letters a, $h^R(a) = h(a)^R$ and $g^R(a) = g(a)^R$, then the PCP (or ωPCP, resp.) can be decided. This extends the class of decidable instances defined here.

Finally, we give another uniqueness property:

UC3. The instance (h, g), where $h, g\colon A^* \to B^*$, is called *unique equality continuation instance*, if, for all $u \in A^*$ and different $a, b \in A$, $h(ua) \bowtie g(ua)$ and $h(ub) \bowtie g(ub)$ imply $h(u) = g(u)$.

We leave the following two questions as open problems: is the PCP decidable for unique equality continuation instances? Is it decidable whether or not an instance of the PCP satisfies the property (UC3)?

Acknowledgements

The first author was Supported by the Academy of Finland under grant 208414. The third author was supported by the Academy of Finland under grant 44087.

References

[1] A. Ehrenfeucht, J. Karhumäki, G. Rozenberg, The (generalized) Post Correspondence Problem with lists consisting of two words is decidable, Theoret. Comput. Sci. 21 (1982) 119–144.
[2] V. Halava, The Post Correspondence Problem for marked morphisms, Ph.D. Thesis, Department of Math., Univ. of Turku, TUCS Dissertations no. 37, 2002.
[3] V. Halava, T. Harju, Infinite solutions of the marked Post Correspondence Problem, in: J. Karhumäki, W. Brauer, H. Ehrig, A. Salomaa (Eds.), Formal and Natural Computing, in: Lecture Notes in Comput. Sci., vol. 2300, Springer-Verlag, 2002, pp. 57–68.
[4] V. Halava, T. Harju, Infinite post correspondence is undecidable for instance of size 9, Theor. Inform. Appl. 40 (4) (2006) 551–558.

[5] V. Halava, T. Harju, M. Hirvensalo, Generalized Post Correspondence Problem for marked morphisms, Internat. J. Algebra Comput. 10 (2000) 757–772.
[6] V. Halava, T. Harju, M. Hirvensalo, Binary (generalized) Post Correspondence Problem, Theoret. Comput. Sci. 276 (2002) 183–204.
[7] V. Halava, T. Harju, J. Karhumäki, Decidability of the binary infinite Post Correspondence Problem, Discrete Appl. Math. 130 (2003) 521–526.
[8] V. Halava, T. Harju, J. Karhumäki, The structure of infinite solutions of marked and binary Post Correspondence Problems, Theory Comput. Syst. 40 (1) (2007) 43–54.
[9] V. Halava, M. Hirvensalo, R. de Wolf, Marked PCP is decidable, Theoret. Comput. Sci. 255 (2001) 193–204.
[10] M.V. Lawson, Finite Automata, Chapman & Hall, 2004.
[11] Y. Lecerf, Récursive insolubilité de l'équation générale de diagonalisation de deux monomorphisms de monoïdes libres $\varphi x = \psi x$, C. R. Acad. Sci. Paris 257 (1963) 2940–2943.
[12] Y. Matiyasevich, G. Sénizergues, Decision problems for semi-Thue systems with a few rules, Theoret. Comput. Sci. 330 (2005) 145–169.
[13] E. Post, A variant of a recursively unsolvable problem, Bull. Amer. Math. Soc. 52 (1946) 264–268.
[14] K. Ruohonen, Reversible machines and Post's correspondence problem for biprefix morphisms, Elektron. Informationsverarb. Kybernet. (EIK) 21 (1985) 579–595.